修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　情報システム学研究科　情報ネットワークシステム学専攻　博士前期課程		
氏　　名	大見　拓也	学籍番号	0952004
論 文 題 目	秘密分散法を用いたコンテンツ配信経路計算法		

要　　旨

コンピュータ間での通信には，データの漏洩や盗聴などの危険性が伴う．情報を安全に保持する方法として，秘密情報を複数のピースに分割して，複数ノードで分散保持する秘密分散法がある．本論文では，秘密分散法によってｋ個に分割されたピースを複数の配信元ノードからｋ本の経路を用いて配信する際に，盗聴に対する安全性が高い配信経路を計算する方法を提案する．

配信元ノードと配信先ノード間のリンクが重複しない経路の最大数をm本とする．この場合，分割されるピースの個数kが幾ら大きくても， m本のリンクを盗聴することによって，全てのピースを盗聴できる．そこで，k本の経路を全て盗聴できるm本のリンクの組み合わせパターン数を最小化するような配信経路の計算法を検討する．この様な配信経路は，整数計画法を用いて定式化し，算出することができる．しかし，整数計画法では計算時間の観点から，大規模ネットワークには適用できない．従って， リンクコストを調整しつつ，ダイクストラ法を用いてk本の経路を逐次的に計算する方法を提案する．

提案方法では，新たな配信経路を算出する際に，既に算出された配信経路が通過するリンクのコストを大きく設定する．これは，新たに算出する経路が，この様なリンクを通過する場合，全ての経路を盗聴できるリンクの組み合わせ数が増加しないためである．更に提案方法では，この様に当該リンクを通過することによって生まれる，全ての経路を盗聴できる，組み合わせ数が増加しないリンクの組み合わせパターン数に応じたリンクコストを設定する．具代的には，当該リンクを通過する既に算出された経路を全て収容しているリンクの数に反比例したリンクコストを設定する．また，提案方法の有効性を示すために，the National Science Foundation（NSF）ネットワークモデルを対象に計算機シミュレーションを行った．

最短経路を計算する整数計画法，すでに算出された配信経路が通過するリンクのコストを一定の大きな値に設定する方法，提案方式に関して計算機シミュレーションによって性能評価を行った．その結果，すべての場合において，提案方式によって得られる組み合わせパターン数は，コストを一定にした方法によって得られるパターン数以下となり，整数計画法を利用して得られる最小値に近づくことを示した．